DORA is now official, are you prepared?

The Digital Operational Resilience Act (DORA) is not only a challenge, but also an opportunity to future-proof your business.

What makes DORA different?

Securing your business is a priority for every organization and DORA imposes a roadmap to do precisely that. The DORA regulation is the cornerstone of the EU's work on digital finance and was introduced with the express purpose of raising the standards for operational resilience across the financial sector. Entities that fall under the regulation will be required to prove that they can withstand, respond to and recover from all types of IT related disruptions and threats. This will carry both challenges and opportunities for your organization.

DORA will extend current requirements for operational resilience by imposing a range of new regulatory obligations including in resilience testing, incident management and reporting. Most notably, DORA will increase the scope of financial regulators supervisory remit so that they will now oversee, and impose requirements upon, the relationship between financial services and their ICT third-party providers. For cloud and ICT service providers this means they will be required to comply with an array of new security and reporting obligations.

Enforcement is envisaged to be managed by European Supervisory Authorities comprised of the European Banking Association (EBA), European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA) respectively. The ESA's will have wide discretion in determining the penalties that they deem necessary to enforce the regulation and in principle they will have all penalty and sanction options open to them.

Five Core Pillars of DORA

ICT risk management
Evidence internal governance and control frame-works that ensure effective management of all ICT risks.

ICT-related incident reporting
Report major incidents to the competent authorities, inform service users and clients.

Digital operational resilience testing
Establish, main-tain, and review digital operational resilience testing programmes.

ICT third party risk
ICT third party risk management including risks arising from contracting third party ICT service providers.

Information sharing
Exchange of cyber threat information and intelligence amongst financial entities.

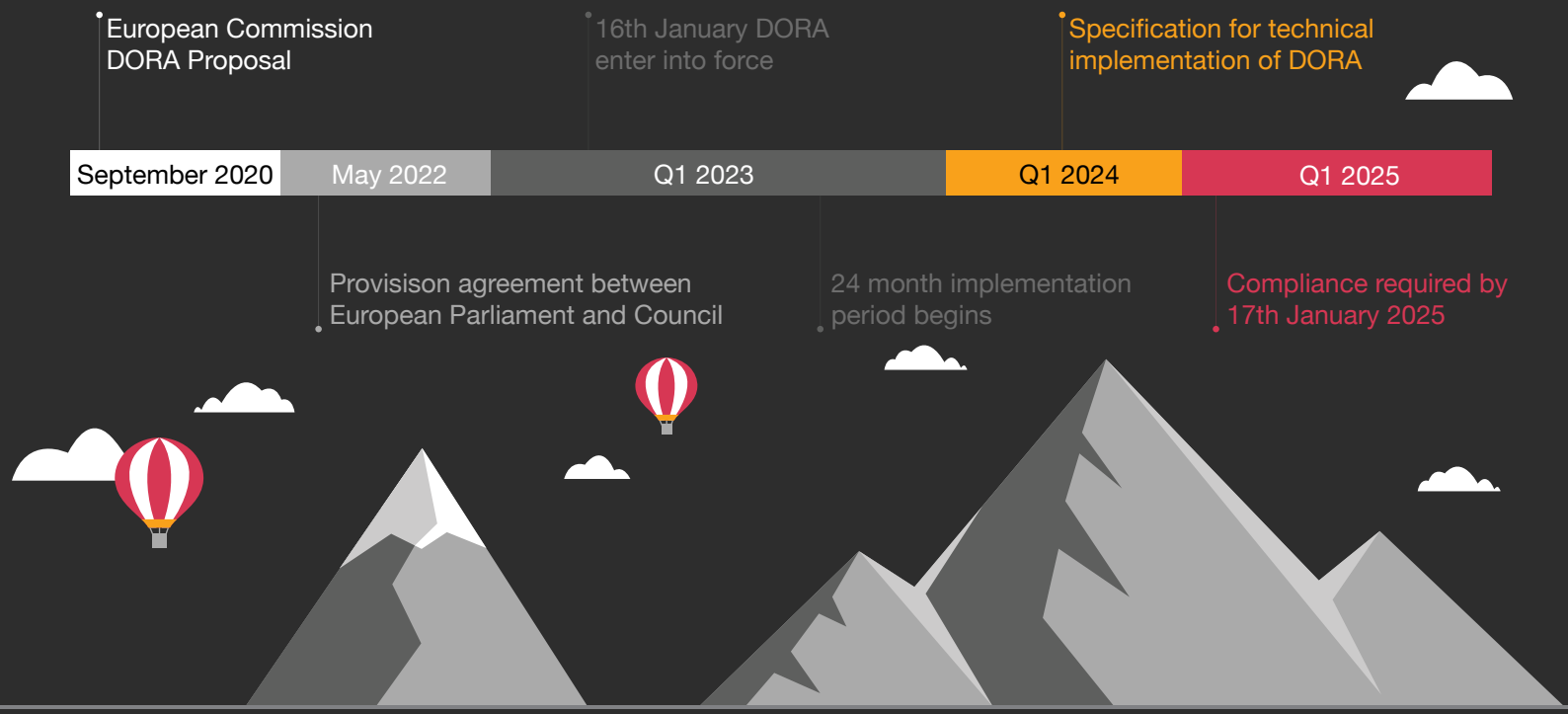
Not only a Challenge but also an Opportunity

Although DORA may seem like a daunting piece of legislation it has the potential to increase maturity across the sector managing ICT risks and dependencies making individual organizations and thus the sector more resilient. DORA is designed to address the full range of your resilience capabilities and help you to foster policies and risk management that will prepare an organization to respond to all forms of threats. Compliance with the regulation will additionally strengthen and streamline resilience exercises both internally and in your supply chain. DORA will stimulate the sharing of threat and intelligence data across financial entities and regularize security expectations of contractual relationships between financial services firms and their third-party ICT providers.

This is an opportunity for you to review your current operational resilience and cybersecurity practices, to streamline these processes which make your business more resilient. This should include:

- Reviewing ICT risk management strategy and your ability to execute on it.
- Preparing your organization for annual testing of critical ICT-systems including through strengthening your ICT asset management and internal digital operational resilience testing.
- Finally, consider the impact of the heightened responsibility and accountability that will be placed on the executive-level.

Now is the time to start



How PwC can help you prepare

Understanding Obligations and Impact Assessment:

- Determine whether your organization is within the scope of DORA and assist you in developing a clear and complete understanding of what the new requirements mean for your organization.
- The next step would be to conduct an impact assessment to determine how the regulation affects you and your current ICT risk framework.

Gap Analysis:

- Assess your current business practices to identify gaps and draft mitigation plans against DORA requirements.

Implementation:

- Ensure you have a holistic approach from ICT risk strategy through execution to deliver on your resilience objective with DORA compliance as an outcome.
- Collaborate with people from Legal, Tax, IT, Audit, Operations, and other departments to achieve compliance with every aspect of DORA.
- Support you to have senior management sufficiently informed on ICT risk topics and certify that mechanisms are in place to report on their decision making.
- Facilitate the development of highly mature ICT asset management which ensures identification and assessment of all assets as a basis for proper ICT risk management.
- Develop your incident handling processes, this may require detailed incident planning, business impact analyses and scenario testing. Scaling up on resources will provide a basis for timely follow-up and reporting to stakeholders on security incidents.
- Enhance your digital operational resilience testing program. Your program should cover all critical IT systems and applications, have a multidimensional security view and a sound risk-based approach.
- Implement an ICT outsourcing approach with a full risk chain perspective which integrates the risks for your organizations ICT outsourcing chain and ensures all potential impacts are known and accounted for.

Compliance:

- Support in adapting your ICT governance, risk framework and outsourcing strategy to ensure it is regulatory, audit and future proof by implementing a data driven approach.

PwC has the skills and expertise to support you

We are able to assist your organization throughout this process. We can offer our insight into the scope of the new regulation, assess the impact to your organization and can accompany you to implement the required ICT-compliance. At PwC we:

Provide operational resilience technology solutions to streamline your implementation and daily cyber efforts.

Support efficient implementation by identifying overlap and synergies between your regulatory compliance obligations (DORA, NIS2, and GDPR).

Take an integrated risk approach to ICT outsourcing by determining the risks associated with your current outsourcing and connecting you to the right ICT outsourcing providers.

Leverage our FS market expertise and experience working with EU regulators to provide relevant insights and prioritized recommendations following a maturity assessment.

Offer a broad market perspective and expert guidance that has been built through experience supporting various financial institutions, fintechs and third-party service providers.

PwC offers multi-disciplinary teams with the depth of experience in technology, cyber security, regulatory compliance and ICT risk management to support you in strengthening your operational resilience, and to help you achieve compliance with the new DORA regulation.

Let's build trust and deliver sustained outcomes for a new tomorrow. This is what we call **The New Equation.**

Who to contact

Anthony Kruizinga
Partner,
Risk & Regulation lead
anthony.kruizinga@pwc.com

Seda Foppen
Director,
IT Risk & Regulation
seda.foppen@pwc.com

Martijn Koopal
Partner,
Legal Services Lead
martijn.koopal@pwc.com

Job van Ommen
Senior Manager,
Cybersecurity & Data Privacy
job.van.ommen@pwc.com

Take a look at our **website.**